REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
12-07-2016	Final Report	12-Aug-2011 - 11-Aug-2015

4. TITLE AND SUBTITLE
Final Report: A Password System Based on Sketches

5a. CONTRACT NUMBER

5b. GRANT NUMBER
W911NF-04-D-0003

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
cliff Wang, Ben Riggins, Wes Snyder

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
North Carolina State University
2701 Sullivan Drive
Admin Srvcs III, Box 7514
Raleigh, NC 27695 -7514

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
60174-MA-SR.2

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Text-based passwords are not necessarily as secure as they appear because the protocols required for a secure password are typically ignored for a more user friendly authentication. We proposed a new sketch-based password system that uses biometric data and provides exceptional trade-off♂ between security and usability. By extending a shape recognition algorithm called Simple K-Space (SKS), a system that is capable of being both secure and robust is developed. In

15. SUBJECT TERMS
Password, biometrics, Human Sketch, identification, classification

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Cliff Wang
UU	UU	UU	UU		19b. TELEPHONE NUMBER 919-549-4207

Report Title

Final Report: A Password System Based on Sketches

ABSTRACT

Text-based passwords are not necessarily as secure as they appear because the protocols required for a secure password are typically ignored for a more user friendly authentication. We proposed a new sketch-based password system that uses biometric data and provides exceptional trade-off♂ between security and usability. By extending a shape recognition algorithm called Simple K-Space (SKS), a system that is capable of being both secure and robust is developed. In theory and experimentation, new insights into the SKS philosophy are provided, including uniqueness of the model and tolerance of the framework. This system is compared with a state-of-the-art graphical password system using Dynamic Time Warping (DTW) and found to achieve comparable performance without using any biometrics.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
08/21/2014	1.00 Zhuo Lu Wenye Wang, Cliff Wang. How Can Botnets Cause Storms? Understanding the Evolution and Impact of Mobile Botnets, , IEEE Info Com 2014. 06-MAY-14, . : ,
TOTAL:	**1**

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
TOTAL:	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper
TOTAL:	

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

SYSTEMS AND METHODS USING DRAWINGS WHICH INCORPORATE BIOMETRIC DATA AS SECURITY INFORMATION

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Ben Riggins	0.50	
Zhu Lu	0.50	
FTE Equivalent:	**1.00**	
Total Number:	**2**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Wesley Snyder	0.00	
Wenye Wang	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**2**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME	
Ben Riggans	
Zhuo Lu	
Total Number:	**2**

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Please see attached report.

Book:
Benjamin S. Riggan, Wesley E. Snyder, Cliff Wang:
Fundamentals of Sketch-Based Passwords - A General Framework. Springer Briefs in Computer Science, Springer 2014, ISBN 978-3-319-13628-8, pp. 1-64

Paper
Benjamin S. Riggan, Wesley E. Snyder, Xiaogang Wang, Jing Feng:
A Human Factors Study of Graphical Passwords Using Biometrics. GCPR 2014: 464-475

Technology Transfer

The created human Sketech based authentication has been demonstrated to Amazon. Potential technology transfer is still being discussed.

A Sketch-based Authentication System with Biometrics: Security and Usability Analysis

Abstract

Text-based passwords are not necessarily as secure as they appear because the protocols required for a secure password are typically ignored for a more user-friendly one. In this paper, we propose a new sketch-based password system that uses biometric data and provides exceptional tradeoff between security and usability. By extending a shape recognition algorithm called Simple K-Space (SKS), a system that is capable of being both secure and robust is developed. In theory and experimentation, new insights into the SKS philosophy are provided, including uniqueness of the model and tolerance of the framework. This system is compared with a state-of-the-art graphical password system using Dynamic Time Warping (DTW) and found to achieve comparable performance without using any biometrics. The addition of biometrics substantially increased the level of performance, reducing the equal error rate (EER) by more than 12%.

Keywords: Security, Authentication, Password, Biometrics, Drawmetrics, Sketches

1. Introduction

In most secured systems, text-based passwords are the golden standard for authenticating users. In theory, traditional passwords are very secure; given

that they meet certain criteria (e.g. randomness, minimum length, and include capital letters, numbers, and special characters). The additional restrictions increase the password strength by increasing size of the *password space*—the total number of possible passwords, which significantly increases the expected number of random guesses required from a brute force attack. In truth, the more random the password, the better. However, a complex password may result in unanticipated consequences:

In reality, users end up breaching the security measures taken by these password systems in one of two ways: 1) constructing a password that is too complex to remember, or 2) ignoring the protocols completely, and creating a simple password. The first scenario is typical of a person who creates a sufficiently complex text-based password, but writes their username and password down (or alternatively saves their login information in a text file called "passwords"). Thus, the security measures taken are essentially nullified. The second case occurs when the security measures are ignored. This case leaves the system vulnerable to a brute force attack because the password space is reduced. Therefore, traditional password mechanisms are not necessarily as secure as they appear.

In recent years, there have been many advancements in the type and number of user authentication methods, including gestures and patterns, picture-based passwords, and biometric recognition schemes. Each approach attempts to optimally balance *security*—preventing unauthorized users from accessing the system—and *usability*—granting access to authorized users with ease. The two extremes for such systems are: 1) perfect security, which does not grant access to anyone, and 2) perfect usability, which grants access to all users. Neither case is desired. Ideally, the only person capable of gaining access should be the genuine user.

In this paper, a new authentication approach, which uses a sketch (or drawing) with biometric information as the form of authentication, is presented. The difficulty with using sketch-based passwords is the stochastic nature of the drawing process. The matching algorithm must be robust enough to handle the variations from the genuine user and simultaneously be secure enough to reject

any forgeries (random or skilled).

Traditional text-based passwords typically use the password space (based on certain assumptions) as the measure for security. However, because password comparisons are more difficult with sketches than with character strings, the password space in this case is not a good measure of security. Therefore we provide both theoretical and empirical evidence that such a password system balances security and usability.

First, a review (Section 2) of previous research related to graphical passwords and biometric systems is discussed. This brief survey provides a summary of alternative graphical passwords and biometric systems. In Section 3, the sketch-based password system is discussed, including enrollment and login phases. In Section 4, we introduce and discuss fundamental theory about the sketch-based password system, including complexity analysis, model uniqueness, and fuzziness (or tolerance). The experiments and results, in Section 5, demonstrate robustness, usability, and security of the sketch-based authentication system. Lastly, conclusions and future work are discussed in Section 6.

2. Related Work

Many researchers have studied and proposed various alternatives to text-based passwords, including using drawings, patterns, gestures [1, 2, 3], pictures and faces [4, 5], and local points or regions [6, 7, 8]. Additionally, biometric recognition methods, such as fingerprint, voice, and facial recognition systems have been recently used for authenticating user access.

2.1. Graphical Passwords

The concept of using graphical passwords has been around for more than a decade. Graphical passwords belong to one of three groups (as proposed in [9]):

1. Drawmetric—recall-based methods
2. Cognometric—recognition-based methods (also referred to as search metric [10])

3. Locimetric—cued-recall based methods.

Drawmetric systems require users to create a distinctive, yet memorable, drawing for a password during enrollment. Then, at login time users are asked to remember their password and accurately reproduce it. This type of system involves a complex human-computer interaction, which includes the conversion from a recalled version of the drawing (stored in the temporal lobe of the brain) to the fully digital representation (stored in a computer's or device's memory). Therefore, a user must physically draw their "password" using a digital tablet or tablet computer (any device with an appropriate user interface for drawing).

The tablet computer market explosion has greatly increased the potential for drawmetric passwords (or password managers). Until now, drawmetric systems have not been able to reach their full potential.

Probably, the most notable drawmetric system is Draw-A-Secret (DAS) [11]. The DAS approach uses a coarse grid, which is displayed to the user, to encode the drawing. The drawing is encoded using the grid cells. The ordered sequence of grid cells that the drawing enters produces a password string. Thus, the matching procedure for DAS is virtually no different from text-based passwords (except for the fact that the string is generated from a drawing); the string produced at login time is compared with the string stored during enrollment.

There are some extensions to DAS which have improved performance. For example, Background Draw-A-Secret [2] improves performance by adding background images. Yet Another Graphical Password (YAGP) [12] improves performance by using a finer grid than the original DAS approach. The result reported include 100% of genuine users being granted access and only 1 security breach in study using 18 participants. By removing the visible grid for drawing and including stroke color as an additional feature, Passdoodle [13, 14] improves performance; [14] achieves around 98% accuracy on a set of 10 users.

One drawback to DAS and similar approaches is the difficulty of encoding near intersection points of grid cells. To alleviate this problem, the Pass-Go [15] approach uses grid intersection points as anchor points instead. Thus,

the encoding records an ordered sequence of horizontal, vertical, and diagonal strokes.

Cognometric systems, instead of drawing, demand that users recognize and select the correct set of images from a randomly assorted set of images. These types of systems leverage the fact that humans tend to recognize something easier than they can remember something. Although cognometric system still require the interaction between a person and a computer, in this case, the procedure is less complicated because the user is not required to produce a drawing. Instead, users are required only to indicate the recognition of a face, landscape, or any other image, using a mouse, keyboard, or touch screen.

The best example of a recognition-based system is PassFaces [5]. During enrollment, the user is presented with a random set of faces and asked to select a subset of them to be their "password." At login time, the user is presented with the correct set of faces dispersed among a random set of other faces. The user is then asked to identify the correct set of faces.

Instead of faces, the Déjà Vu [4] system uses a set of images with patterns and art. Studies [16, 17] have shown that, even with choosing faces, people are predictable in their choice of password. Déjà Vu attempts to alleviate this problem by making the images very randomized, so that a bias or preference toward any particular image is less likely to occur.

Locimetric systems, instead of requiring users to remember entire images, have users recall and identify specific points or regions within an image. The idea is to reduce the amount of information that a user is required to remember. Given a larger image, a user selects an ordered sequence of points or regions located within the image. In principle, the image should help stimulate the process of remembering the points previously chosen, hence the term cued-recall.

The most prominent cued-recall based method is PassPoints [6, 7, 8]. PassPoints presents the user with a single image, typically having numerous landmarks: people, buildings, objects, etc., from which the user is supposed to select 5 different locations during enrollment. At login time, the user is again presented with the same image, and the user must choose the correct set of points within

the image in precisely the same order.

An extension to the PassPoints philosophy, called Cued Click-Points [18, 19], presents the user with multiple images (one at a time). In each image the user selects only one point to use. Similarly, the ordered sequence of locations in each image becomes the password. If any one point is incorrect, access is denied.

Many of the methods using drawmetric, cognometric, and locimetric password systems are compared and contrasted in [20]. This literature survey analyzes the multitude of methods in terms of both usability and security, especially the vulnerabilities to different attacks (e.g. brute force, phishing, and shoulder surfing).

2.2. Biometric Systems

Biometric systems—systems that measure and analyze certain biological properties for the purposes of identity recognition [21]—are steadily becoming a part of everyday life, including in commercial access systems, personal computers, and smart phones. Biometrics are increasingly popular because they are supposed to be universal, distinct, permanent, and collectible [22] properties that uniquely identify an individual. For these reasons, biometrics are considered much more secure than traditional passwords.

Biometrics include biological properties such as fingerprints, voices, faces, and even handwriting. Fingerprints have been widely used and accepted in forensic, commercial, government security, and consumer applications. Despite the fact that fingerprints are essentially unique to every individual, there are still concerns in terms of a system's ability to recognize fingerprints (especially with consumer applications). For example, fingerprint recognition is very sensitive to noise and partial occlusion. In most cases, the signal-to-noise ratio (SNR) is low, which increases the difficulty of recognizing fingerprints accurately (implying the possibility of a breach in security).

Occlusion also presents a problem for fingerprint recognition because the fingerprint (and its features) must be visible (at least mostly visible) in order to determine with sufficient confidence that it matches another fingerprint. There

are several reasons for occlusion of a fingerprint including varying poses and pressure.

Voice recognition systems, although not as widely used as fingerprint recognition in security applications, are used in applications such as voice-to-text in cars (e.g. Ford Sync) and smart phones (e.g. Apple's Siri), and voice command systems (e.g. Microsoft Xbox). There are many reliability concerns when it comes to voice recognition systems for user authentication. Multiple variables, such as distance to microphone(s), background noise, and vocal anomalies (e.g. colds, dialects, and accents), affect the reliability of a voice recognition system. The most disturbing of these variables are the anomalies because they naturally occur in human voices, but voice recognition systems still experience difficulty in handling these effects.

Facial recognition systems for authenticated access are also becoming more common because of advancements with this technology. However, there are still some concerns about the reliability of these systems. Facial recognition most commonly experiences difficulties with occlusion. Faces can be occluded because of clothing or accessories, lighting conditions, or even pose. As with fingerprints, the confidence of the face recognition is reduced when there is occlusion. Under normal operating conditions, one would expect facial recognition to perform quite well. However, there are legitimate security concerns for false acceptances—when the system grants access to an unauthorized person.

Although it is difficult, under normal conditions, to change or alter a person's fingerprint, voice, or face, it certainly plausible that an authorized user may be coerced (with extreme force) into unlocking the system, thus, granting access to unauthorized users. In addition, a fingerprint can be reproduced (or in the extreme case a finger can be severed), a voice may be recorded or copied, and a face recognition system can be fooled with a picture of a face. Each of these measures requires going to great lengths, but all are reasonable means to fool a biometric system. For sketch-based passwords, we believe that a coerced user is less likely to reproduce a sketch accurately enough to gain access to the system because of additional nervous jitter while under duress. However, this is not

considered in this work.

According to Jain et. al, "foolproof personal recognition systems simply do not exist and perhaps, never will" [22]. However, in this paper, we attempt to introduce a new system that bridges the gap between security and usability.

3. Recognizing Sketch-based Passwords

In this section, the biometric sketch-based password system is discussed. The method used for recognizing sketch-based passwords with biometric information in essence works by first constructing a descriptor or a model, and then applying a matching procedure that looks for consistency between a sketch and this model.

In password systems, typically the terms recognition and/or matching are implied to mean *verification*—the problem of confirming that a user is indeed who he/she claim to be—which is also the implication in this paper.

3.1. Overview

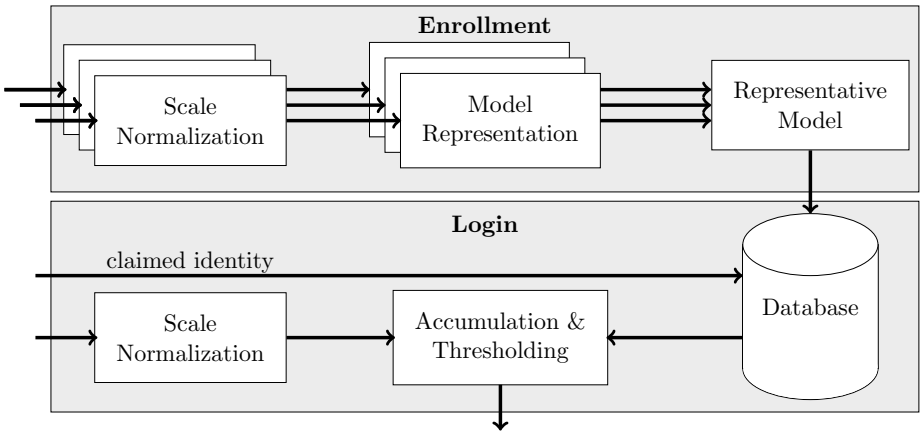


Figure 1: The diagram depicts the primary components of both the enrollment and login phases for the proposed sketch-based password system. The inputs (depicted with arrows) to the "Scale Normalization" blocks for both *enrollment* and *login* represent the input sketches from the user for the respective phases.

There are two primary phases which are used in a sketch-based password system:

1. Enrollment—User registers using a username and sets his/her sketch-based password.
2. Login—User enters his/her username and draws an instance of the password.

Fig. 1 outlines the major procedures necessary for both enrollment and login phases. The diagram shows two important steps involved within each phase: capturing the input sketches and normalizing the scale. The next step for enrollment is constructing the model for each normalized sketch, from which a representative model for the class of acceptable sketch-based passwords is produced. This representative model is then stored in the user database.

After normalizing the input sketch during the login phase, the model for the claimed user identity is retrieved from the database. Then, the consistency between the model and the sketch are determined using an accumulative method. If enough evidence exists for the sketch to be considered similar to the exemplar sketches that constructed the model, then access is granted. Otherwise, access is denied.

3.2. Input and Normalization

The input of the sketch-based password system is simply a sketch. More rigorously, a parameterized sketch (excluding biometrics for now) is considered to be a continuous mapping $\boldsymbol{\alpha}\colon I \to \mathbb{R}^2$, expressed as $\boldsymbol{\alpha}(s) = (x(s), y(s))$ for arc length $s \in I$, where I is the interval $(0, 1)$ without loss of generality.

Given a sketch, the scale, according to Kendall's [23] definition, is proportional to the average distance from the center of gravity. In order to achieve scale invariance, every sketch is normalized to unity scale. Therefore, the recognition does not depend on the size of the sketch. Note that this particular definition of scale is only useful for non-occluded shapes or curves. In the application of sketch-based passwords, occluded sketches are considered to be different or incomplete passwords. Therefore, occlusion is not considered in this paper.

3.3. Enrollment

During enrollment, the user is expected to provide multiple instances of the sketch-based password. Multiple sketches are required in order to construct a model which is more accurate and robust than a model produced by a single sketch. The main idea is to capture more of the possible variations from a particular user, which helps to produce a model that is consistent with sketch-based passwords generated by that particular user. This is, in fact, similar to traditional text-based schemes. In most text-based password systems, users are required to enter their desired password at least twice. Therefore, it is not unreasonable for a sketch-based password system to demand multiple sketches during enrollment. Due to the additional complexity of a sketch compared with an alphanumeric string, it is reasonable that a sketch would require more than two examples for enrollment (e.g. 3–5).

Given a normalized sketch, the goal is to construct a model or descriptor that captures the desired properties of a sketch, which include:

- shape (e.g. relative distance and curvature)
- drawing direction (e.g. sketch tangent direction)
- biometrics (e.g. pressure, velocity, or acceleration)
- parametrization (e.g. time or arc length).

The model we have chosen is a biometric extension and generalization of a shape recognition approach called Simple K-Space (SKS) [24, 25]. A generalization of SKS is implemented because it has been shown to be robust to the multitude of variations to shape contours [26]. Since a sketch for all intents and purposes is considered to be a shape, an extension to SKS which models shape and other properties seemed appropriate.

Before discussing the model construction, several local features of the sketch are required. These features are intended to capture the local properties discussed above.

Two shape functions, $\rho_{\boldsymbol{\alpha}}(s)$ and $\kappa_{\boldsymbol{\alpha}}(s)$, are computed (or estimated) from the normalized sketch, $\boldsymbol{\alpha}(s)$. $\rho_{\boldsymbol{\alpha}}(s) = \|\boldsymbol{\alpha}(s) - \mathbf{x}_0\|$ is defined as the Euclidean distance between the spatial coordinates at arc length s along the sketch, $\boldsymbol{\alpha}(s)$, and an arbitrary, but constant spatial reference point, $\mathbf{x}_0$. In this approach, we have chosen the reference point of the sketch to be the center of gravity. $\kappa_{\boldsymbol{\alpha}}(s)$ is defined as the local curvature at the point s on the sketch. Curvature is defined as the magnitude of the derivative to the unit tangent vector, or $\kappa(s) = |T'(s)| = |\boldsymbol{\alpha}''(s)|$.

Typically, $\rho_{\boldsymbol{\alpha}}(s) \in U$ and $\kappa_{\boldsymbol{\alpha}}(s) \in K$, where $U \subset \mathbb{R}$ is defined by $[0,\ \rho_{max}]$ and $K \subset \mathbb{R}$ is defined by $[0, \kappa_{max}]$. In practice, ρ_{max} and κ_{max} are determined respectively by the length of the diagonal of the active drawing area (x-y plane) and the device resolution.

Note that both features, distance and curvature, are invariant to translation, rotation, and reflections.

In order to capture the drawing direction at each point along the sketch, $\boldsymbol{\alpha}(s)$, the tangent direction to the sketch is computed. The tangent direction at a point s along the sketch is represented by a scalar angle $\theta_{\boldsymbol{\alpha}}(s) \in \Theta$, where $\theta_{\boldsymbol{\alpha}}(s) = \text{atan2}(y'(s), x'(s))$ and Θ is defined by the interval $(-\pi, \pi]$.

Since sketches drawn by most users are very noisy (in terms of jitter caused by shaking of the hand), $\theta_{\boldsymbol{\alpha}}(s)$ is significantly impacted by the amount of jitter. There are two ways to handle jitter in the drawing direction: 1) quantizing the direction angle, and 2) smoothing the jitter using a convolution kernel. In our approach, we use the latter approach because noise near a quantization level boundary introduces significant errors. The direction feature is not smoothed directly, however, SKS includes a parameter that blurs all features (not just direction) in order to be more robust.

The next property of a sketch that is modeled is the biometric component—pressure—which is denoted by the function $b_{\boldsymbol{\alpha}}(s)$. The pressure, $b_{\boldsymbol{\alpha}}(s) \in B$, is a scalar measurement representing the amount of force applied by the pen with the active area on the device's screen, where B is defined as the interval $[0,\ 1]$.

Finally, the arc length, $s_{\boldsymbol{\alpha}}(t) = \int_0^t \|\boldsymbol{\alpha}(u)\|\ \mathrm{d}u$, is used as a feature. The

arc length is used primarily to impose a general ordering of the samples of the sketch (i.e. how a sketch is drawn). However, it also significantly improves performance. The arc length without loss of generality is on the interval S, defined by $[0,\ 1]$.

After computing each of the functions: $\rho_{\boldsymbol{\alpha}}(s)$, $\kappa_{\boldsymbol{\alpha}}(s)$, $\theta_{\boldsymbol{\alpha}}(s)$, $b_{\boldsymbol{\alpha}}(s)$, and $s_{\boldsymbol{\alpha}}(t)$, the model of a sketch, $\boldsymbol{\alpha}(s)$, is defined as:

$$m_{\boldsymbol{\alpha}}(\mathbf{v}) = \frac{1}{z}\int_0^1 \exp\left(-\frac{1}{2}(\mathbf{v}-\mathbf{v}_{\boldsymbol{\alpha}}(\tau))^T\boldsymbol{\Sigma}^{-1}(\mathbf{v}-\mathbf{v}_{\boldsymbol{\alpha}}(\tau))\right)\,\mathrm{d}\tau \tag{1}$$

where $\mathbf{v}_{\boldsymbol{\alpha}}(\tau) = [\rho_{\boldsymbol{\alpha}}(\tau)\ \kappa_{\boldsymbol{\alpha}}(\tau)\ \theta_{\boldsymbol{\alpha}}(\tau)\ b_{\boldsymbol{\alpha}}(\tau)\ s_{\boldsymbol{\alpha}}(\tau)]^T$ is the local feature vector at the point τ on the sketch (and τ is just a "dummy" arc length variable), z is a normalization factor (see Section 3.5), and $\boldsymbol{\Sigma}$ is the covariance matrix used for smoothing the model. The intent behind blurring the model is to make the matching of a sketch more robust during the login phase (Section 3.4). This is discussed further in Section 4.3.

In this work, $\boldsymbol{\Sigma}$ is assumed to be a diagonal covariance matrix that is constant over all sketches. The non-zero parameters in the matrix are determined experimentally. However, in general, a diagonal $\boldsymbol{\Sigma}$ is not necessary.

The model in Eq. (1), $m_{\boldsymbol{\alpha}}\colon \mathcal{F} \to \mathbb{R}$, is a scalar function defined for all vectors $\mathbf{v} = [\rho, \kappa, \theta, b, s]^T \in \mathcal{F}$, where $\mathcal{F} \subset U \times K \times \Theta \times B \times S$. The scalar value represents a *likelihood* that there exists a point, at an arc length of s on $\boldsymbol{\alpha}$, that is a distance of ρ from the reference, has a curvature of κ, has a drawing direction of θ, and has a pressure of b .

The model, in fact, may be viewed as a hyper-surface defined over $\mathcal{F} \subset \mathbb{R}^5$, and it very much resembles a kernel density estimator [27]. However, the main difference is the normalization factor, z. Density estimators normalize such that

$$\int_{\mathcal{F}} m_{\boldsymbol{\alpha}}(\mathbf{v})\ \mathrm{d}\mathbf{v} = 1,$$

instead, an alternative method of normalization, which is better suited to this application, is used (Section 3.5).

After constructing each model for the multiple sketches drawn by the user during the enrollment stage, it is useful to construct a single representative

model (opposed to matching with all exemplars). This is accomplished by averaging the set of models. At first this approach may appear to be trivial, however, the reason behind it is not intuitive. The assumption is that sketches input by the user during enrollment must be *similar* sketches. This means the sketches must be of the same shape and drawn in a similar manner. Therefore, on the manifold of sketches, they are considered to be "close" in term of their geodesic distance. Since the models are constructed from these sketches, they too lie in "close" proximity on the manifold of models. The average is then an excellent representative model for the class because manifolds are locally linear and the average optimally minimizes the distance from each point in a linear space. However, if a user enters extremely different sketches during enrollment then the average model is a poor representative of the set of sketches. A simple outlier test to determine if the sketches provided by the user during enrollment are sufficiently different is implemented.

An interesting observation is that the optimal sketch necessary to produce the representative model is unknown to the user after enrollment, unless the user is perfectly consistent (practically impossible). However, as individuals use this system by logging in with a sketch, they adapt and learn what the system expects to be a "correct" sketch, which is significantly easier if one is the genuine user and already know what was drawn and how it was drawn. Although this not the primary focus of this paper, it is an interesting process that occurs during the human-computer interaction.

Now that the enrollment phase has been discussed, we move on to discuss the login phase which is the primary mode of operation.

3.4. Login

During the login phase, a user inputs his/her putative identity using a username or pin, and then the user draws the sketch-based password (attempting to replicate the underlying biometric signature used during enrollment). This sketch is then determined to be either sufficiently or insufficiently consistent with the representative model of the putative user.

The method used for computing this measure of consistency is a higher dimensional extension of the matching procedure used by SKS. The SKS approach uses an accumulative framework for determining the consistency of a shape with a shape model. Thus, the approach used here is very similar for sketches.

Given a login sketch, $\boldsymbol{\alpha}_\ell(s) = (x_\ell(s),\ y_\ell(s))$ (with corresponding curvature, direction, pressure, and arc length functions) and model $m_{\boldsymbol{\alpha}}(\mathbf{v})$, the accumulator is defined as

$$A(\hat{\mathbf{x}}) \equiv acc_{\boldsymbol{\alpha},\boldsymbol{\alpha}_\ell}(\hat{\mathbf{x}}) = \int_0^1 m_{\boldsymbol{\alpha}}(\mathbf{v}_{\boldsymbol{\alpha}_\ell}(\tau, \hat{\mathbf{x}}))\ \mathrm{d}\tau \tag{2}$$

where

$$\mathbf{v}_{\boldsymbol{\alpha}_\ell}(\tau, \hat{\mathbf{x}}) = [\|\hat{\mathbf{x}} - \boldsymbol{\alpha}_\ell(\tau)\|\ \kappa_{\boldsymbol{\alpha}_\ell}(\tau)\ \theta_{\boldsymbol{\alpha}_\ell}(\tau)\ b_{\boldsymbol{\alpha}_\ell}(\tau)\ s_{\boldsymbol{\alpha}_\ell}(\tau)]^T$$

is the feature vector defined by $\boldsymbol{\alpha}_\ell$ and $\hat{\mathbf{x}}$; $A(\hat{\mathbf{x}})$ represents the likelihood that $\hat{\mathbf{x}} = (\hat{x}, \hat{y})$ is the reference point of the sketch, $\boldsymbol{\alpha}_\ell$. This likelihood may be considered to be the result from a path integral over the hyper-surface of the model, $m_{\boldsymbol{\alpha}}$, where the path is defined by $\hat{\mathbf{x}}$ and the local features of the login sketch. An example of this path integration using a 2D model (higher dimensional cases are more difficult to illustrate) is shown in Fig. 2.

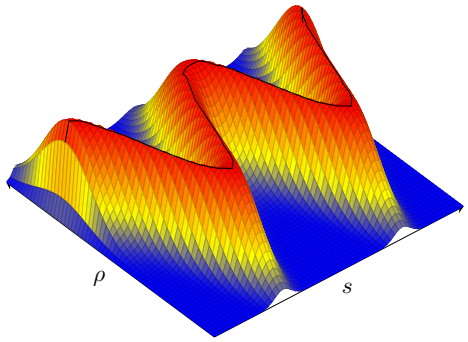
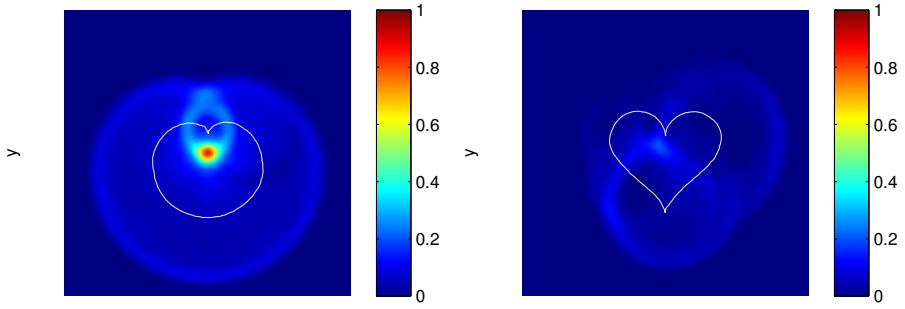


Figure 2: The surface represents the model constructed over the ρ-s feature space, and the line represents an integration path defined by $\hat{\mathbf{x}}$ and the features of $\boldsymbol{\alpha}_\ell$. The result from each integral path represents the likelihood that $\hat{\mathbf{x}}$ is the reference point for the model sketch.

Assuming that $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}_\ell$ are, indeed, two similar sketches, the consistency measure increases as $\hat{\mathbf{x}}$ approaches the actual reference point of $\boldsymbol{\alpha}_\ell(s)$. The result is a global maximum in the accumulator at the location of the "best" reference point. On the other hand, if $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}_\ell$ are sufficiently different, no significant peak will occur. However, the accumulator may have other local maxima; their amplitudes are usually small in comparison to that of a peak generated from a similar sketch. Fig. 3 shows the difference between matching and non-matching accumulators.



(a) (b)

Figure 3: Example of an accumulator that indicates a sketch (shown on top of the accumulator) that is consistent with the model (a), and an accumulator that indicates a different sketch (also shown) is inconsistent with the same model (b).

Since the amplitude at every point in the accumulator represents the likelihood measure for that point being the reference point, then the best reference point occurs at $\mathbf{x}^* = \arg\max_{\mathbf{x}} A(\mathbf{x})$. Thus, the authentication decision is made as follows:

$$decision = \begin{cases} \text{Access Granted}, & A(\mathbf{x}^*) > Thresh \\ \text{Access Denied}, & A(\mathbf{x}^*) \leq Thresh \end{cases}$$

which means that if the login sketch, $\boldsymbol{\alpha}_\ell$, is sufficiently consistent (the accumulator peak is greater than than the threshold, $Thresh$) with the model for $\boldsymbol{\alpha}$, then the two sketches are considered to be similar.

3.5. Model Normalization

Normalizing the model, although not a necessity, makes determination of sketch consistency with a model much easier. Consider the unnormalized model (i.e. where $z = 1$) for the sketch $\boldsymbol{\alpha}(s)$

$$\tilde{m}_{\boldsymbol{\alpha}}(\mathbf{v}) = \int_0^1 \exp\left(-\frac{1}{2}(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau))^T \boldsymbol{\Sigma}^{-1}(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau))\right) \, \mathrm{d}\tau. \tag{3}$$

The sketch which is most consistent with $\tilde{m}_{\boldsymbol{\alpha}}$ is $\boldsymbol{\alpha}(s)$. Therefore, the normalization factor

$$z = \int_0^1 \tilde{m}_{\boldsymbol{\alpha}}(\mathbf{v}_{\boldsymbol{\alpha}}(\tau, \mathbf{x}^*)) \, \mathrm{d}\tau, \tag{4}$$

which represents the result of integrating on the path (defined by the best reference point $\mathbf{x}^*$) over the unnormalized model. Using this definition of z, the model is normalized such that $acc_{\boldsymbol{\alpha},\boldsymbol{\alpha}}(\mathbf{x}^*) = 1$ (i.e. the consistency between the model of $\boldsymbol{\alpha}(s)$ and $\boldsymbol{\alpha}(s)$ itself is maximal). In practice, this means if a sketch is consistent with the model, then the magnitude of the peak in the accumulator should be close to one. Otherwise, it should be bounded away from one. How far below one depends on the severity of the deformation from the original sketch. The more deformed the sketch, the smaller the peak in the accumulator. Therefore, normalizing the model in this manner simplifies the process of determining the consistency of the match.

4. Discussion and Analysis

In this section, various properties and theorems are discussed, including duality and computational complexity of constructing a model, uniqueness of a model, and fuzziness in the accumulator. Every claim introduced here is crucial for showing that the sketch-based password system is robust, secure, and efficient.

4.1. Duality and Computational Complexity

One important property of SKS is the duality for building a model of a sketch. The direct implementation as expressed in Eq. (1) is called the primal form, and it is implemented in Algorithm 1.

Algorithm 1 Primal

for $\mathbf{v} \in \mathcal{F}$ **do**

  for $\tau \in [0, 1]$ **do**

    $m_{\boldsymbol{\alpha}}(\mathbf{v}) \leftarrow m_{\boldsymbol{\alpha}}(\mathbf{v}) + \exp\left(-\frac{1}{2}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)^T \boldsymbol{\Sigma}^{-1}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)\right)$

  end for

end for

There also exists a dual to the primal algorithm, in which the curve is only iterated over once rather than multiple times (as with the primal form). The dual is outlined in Algorithm 2

Algorithm 2 Dual

for $\tau \in [0, 1]$ **do**

  for $\mathbf{v} \in \mathcal{F}$ **do**

    $m_{\boldsymbol{\alpha}}(\mathbf{v}) \leftarrow m_{\boldsymbol{\alpha}}(\mathbf{v}) + \exp\left(-\frac{1}{2}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)^T \boldsymbol{\Sigma}^{-1}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)\right)$

  end for

end for

Both primal and dual algorithms implement the same integrals, but the manner in which the integrals are computed distinguishes them from one another. The primal form computes the model by integrating over the sketch for every point, $\mathbf{v}$, in the model. However, the dual only iterates over the model for every point along the sketch. Note the subtle distinction and that both primal and dual have exactly the same algorithmic complexity. However, the dual can be used to construct an approximate model more efficiently, as we explain below.

The dual form (Algorithm 2) provides a way to efficiently construct a good approximation of the model. For each point on the sketch, every point $\mathbf{v}$ is updated in the model by a factor: $\exp\left(-\frac{1}{2}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)^T \boldsymbol{\Sigma}^{-1}\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)\right)$. This factor represents a Gaussian centered at some location in the model, which is defined by the local features on the sketch, denoted by $\mathbf{v}_{\boldsymbol{\alpha}}(\tau)$. Therefore, only points in the model that are within a reasonable local neighborhood of the center of this Gaussian need updating, which significantly reduces the computational

complexity for computing the model. Using a finite region of support for the Gaussian, we can show that dual algorithm scales linearly with the number of points along the sketch (Observation 1).

Observation 1. *The complexity for constructing the model is $\mathcal{O}(p)$, where p is the number of samples along the sketch.*

Proof. For each of the p points along the sketch, every point inside the local neighborhood of the corresponding features of p is updated. Thus, the computational complexity is $\mathcal{O}(p\mathcal{N}_p)$ where $\mathcal{N}_p$ denotes the size of the neighborhood or region of support. Assuming that the neighborhood size, defined by the set of points inside the $2\boldsymbol{\Sigma}$ or $3\boldsymbol{\Sigma}$ hyper-ellipsoid, is fixed for all p, then $\mathcal{N}_p$ is constant and the complexity scales linearly with the number of samples over the sketch. Therefore, the complexity reduces to $\mathcal{O}(p)$. □

4.2. Model Uniqueness in the Limit

An interesting result of using the SKS model (Eq. (1)) is the property of having a unique model (in the limit). This comes primarily from the intuition behind the shape recognition model, but it is also applicable to the generalization discussed in this paper.

Consider the limit of the SKS model of a parameterized curve as the elements of the positive definite matrix $\boldsymbol{\Sigma}$ approach 0 (i.e. $\boldsymbol{\Sigma} \to \mathbf{0}$ where $\mathbf{0}$ is the matrix with all zero elements)[1]:

$$\lim_{\boldsymbol{\Sigma}\to\mathbf{0}} m_{\boldsymbol{\alpha}}(\mathbf{v}) = \frac{1}{z}\int_0^1 \delta\left(\mathbf{v} - \mathbf{v}_{\boldsymbol{\alpha}}(\tau)\right)\, \mathrm{d}\tau$$

where

$$\delta(\mathbf{x}) = \lim_{\boldsymbol{\Sigma}\to\mathbf{0}} \exp\left(-\frac{1}{2}\mathbf{x}^T\boldsymbol{\Sigma}^{-1}\mathbf{x}\right) = \begin{cases} 1, & \mathbf{x} = \mathbf{0} \\ 0, & \mathbf{x} \neq \mathbf{0} \end{cases}$$

Now, consider a mapping $\psi\colon \mathcal{S} \to \mathcal{M}$ (defined by the model), which maps an element of $\mathcal{S}$—the "space of sketches"—to the "space of models," $\mathcal{M}$. Note

[1] $\lim_{\boldsymbol{\Sigma}\to\mathbf{0}} \boldsymbol{\Sigma} \equiv \lim_{\zeta\to 0} \zeta\boldsymbol{\Sigma}$

the distinction between $m_{\boldsymbol{\alpha}}(\mathbf{v})$, which maps an element of $\mathcal{F}$ to $\mathbb{R}$, and ψ, which maps a "sketch" to some hyper-surface defined by $(\mathbf{v}, m_{\boldsymbol{\alpha}}(\mathbf{v}))$ in $\mathcal{M}$.

Here, we show that the mapping ψ is a one-to-one mapping in the limit, which implies the smoothing matrix $\boldsymbol{\Sigma}$ may be used to set the trade-off between a unique model or tolerant model (i.e. security vs. usability).

Theorem 1. *In the limit as $\boldsymbol{\Sigma} \rightarrow \mathbf{0}$, two models $\psi(\boldsymbol{\alpha}_1)$ and $\psi(\boldsymbol{\alpha}_2)$ of two sketches, $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_2$ respectively, are equal iff $\boldsymbol{\alpha}_2 = T_{iso}(\boldsymbol{\alpha}_1)$, where T_{iso} is some isometry (e.g. translation, rotation, or reflection).*

In order to prove Theorem 1, the following lemma is necessary.

Lemma 1. *Given that the feature vector $\mathbf{v}(s)$ at s is invariant to any isometry, then $\mathbf{v}_1(s)$=$\mathbf{v}_2(s)$ iff $\boldsymbol{\alpha}_2 = T_{iso}(\boldsymbol{\alpha}_1)$.*

Proof. First, we need to make sure that the assumption about the feature vectors holds. In the case for sketches, ρ which is a distance from the center of gravity is invariant to translation, rotation, and reflection; as is the curvature κ. The tangent direction θ is not directly invariant to rotation or reflection. However, the angle can be measured relative to the principle direction (which rotates and reflects with the sketch). Therefore, θ may also be invariant to isometries. The biometric b is also invariant to isometries because it translates, rotates, and reflects with the sketch, and arc length is also invariant. Therefore, with sketches we may ensure that the features are invariant to any isometry.

Assuming that $\boldsymbol{\alpha}_2 = T_{iso}(\boldsymbol{\alpha}_1)$, then due to the invariance to isometries $\mathbf{v}_1(s)$=$\mathbf{v}_2(s)$. And if $\mathbf{v}_1(s)$=$\mathbf{v}_2(s)$, then $\boldsymbol{\alpha}_2$ is equal to $\boldsymbol{\alpha}_1$ (up to a rigid transformation). □

Now, we can prove Theorem 1.

Proof. Assume that $\boldsymbol{\alpha}_2 = T_{iso}(\boldsymbol{\alpha}_1)$. From *Lemma* 1, this implies that $\mathbf{v}_1(s)$=$\mathbf{v}_2(s)$.

Therefore,

$$\begin{aligned}\lim_{\boldsymbol{\Sigma}\to\mathbf{0}} m_{\boldsymbol{\alpha}_1}(\mathbf{v}) &= \frac{1}{z}\int_0^1 \delta\left(\mathbf{v}-\mathbf{v}_{\boldsymbol{\alpha}_1}(\tau)\right)\ \mathrm{d}\tau \\ &= \frac{1}{z}\int_0^1 \delta\left(\mathbf{v}-\mathbf{v}_{\boldsymbol{\alpha}_2}(\tau)\right)\ \mathrm{d}\tau \\ &= \lim_{\boldsymbol{\Sigma}\to\mathbf{0}} m_{\boldsymbol{\alpha}_2}(\mathbf{v}).\end{aligned}$$

Thus, $\psi(\boldsymbol{\alpha_1}) = \psi(\boldsymbol{\alpha_2})$.

Conversely, we want to show that $\psi\left(\boldsymbol{\alpha}_1\right) = \psi\left(\boldsymbol{\alpha}_2\right)$ implies $\boldsymbol{\alpha}_2 = T_{iso}(\boldsymbol{\alpha}_1)$. However, if the contrapositive:

$$\boldsymbol{\alpha}_2 \neq T_{iso}(\boldsymbol{\alpha}_1) \Rightarrow \psi\left(\boldsymbol{\alpha}_1\right) \neq \psi\left(\boldsymbol{\alpha}_2\right)$$

is true, then the original statement itself is also true.

So, assuming that $\boldsymbol{\alpha}_2 \neq T_{iso}(\boldsymbol{\alpha}_1)$, then we know that $\mathbf{v}_1(s) \neq \mathbf{v}_2(s)$ from Lemma 1. Therefore, $\exists s^*$ s.t. $\mathbf{v}^* = \mathbf{v}_1(s^*) \neq \mathbf{v}_2(s^*)$. Then, it follows that:

$$\begin{aligned}\lim_{\boldsymbol{\Sigma}\to\mathbf{0}} m_{\boldsymbol{\alpha}_1}(\mathbf{v}^*) &= \frac{1}{z}\int_0^1 \delta\left(\mathbf{v}^*-\mathbf{v}_{\boldsymbol{\alpha}_1}(\tau)\right)\ \mathrm{d}\tau \\ &= \frac{1}{z}\delta\left(\mathbf{v}^*-\mathbf{v}_{\boldsymbol{\alpha}_1}(s^*)\right) = \frac{1}{z}\end{aligned}$$

and

$$\begin{aligned}\lim_{\boldsymbol{\Sigma}\to\mathbf{0}} m_{\boldsymbol{\alpha}_2}(\mathbf{v}^*) &= \frac{1}{z}\int_0^1 \delta\left(\mathbf{v}^*-\mathbf{v}_{\boldsymbol{\alpha}_2}(\tau)\right)\ \mathrm{d}\tau \\ &= \frac{1}{z}\delta\left(\mathbf{v}^*-\mathbf{v}_{\boldsymbol{\alpha}_2}(s^*)\right) = 0\end{aligned}$$

Thus, $\psi(\boldsymbol{\alpha_1}) \neq \psi(\boldsymbol{\alpha_2})$. □

This concept of uniqueness does not theoretically hold for arbitrary $\boldsymbol{\Sigma}$. However, the system is designed intentionally so that there is some level of tolerance—*non-uniqueness*—in the model. This is due to the fact that people are not perfect; they make errors when reproducing a sketch. So, in order to make the system more robust and usable, the model is intentionally fuzzy and not unique. In fact, true uniqueness is not desirable.

Intuitively, we are claiming that, in general, uniqueness is only a local property of the model. We provide some experimental evidence to support this claim in Section 5.1.

4.3. Robustness in the Accumulator

Given a model $m_{\boldsymbol{\alpha}}(\mathbf{v})$, there exists some continuous path $\mathbf{p}$ (Fig. 2) over the model, that is the $\boldsymbol{p}$ is defined in terms of the features, that maximizes the peak in the accumulator (Eq. (2)). In principle, this path is defined by $\boldsymbol{\alpha}$. Therefore, there exists a small "band" or "tube" around the path $\mathbf{p}$ that defines allowable deviation from the optimal path (corresponding to deviations of the sketch) over the model, which results in a "small" difference in the accumulator peak.

Primarily due to jitter and other noise factors while drawing, most people cannot perfectly reproduce their own sketch. A significant (but less than optimal) amount of accumulation occurs when a sketch, corresponding to a near optimal path over the model, is drawn. Therefore, there is some amount of tolerance (i.e. robustness) built directly into the matching procedure. This tolerance, which is also controlled by $\boldsymbol{\Sigma}$, is what makes this system more practical. Thus, more blurring in the model implies less security of the system because less accuracy is required of the user.

5. Experiments and Results

In this section, we demonstrate the feasibility and security of our system through experimentation. In order to demonstrate the current level of performance, several experiments are performed using both synthetic and hand-drawn sketches. The purpose of these experiments is two-fold: 1) to support the claims in Section 4 and 2) to provide a performance analysis of the proposed password system.

In this paper, as well as many other biometric systems, performance is measured by the false acceptance rate (FAR) versus the false rejection rate (FRR) curve. The FAR is the number of accepted forgeries divided by the total number of forgeries, and the FRR is the number of genuine sketches that are rejected divided by the total number of genuine sketches. In some cases, performance is reported with a single number referred to as the equal error rate (EER), which is the rate where the FAR and FRR are equal.

5.1. Model "Uniqueness"

In this set of experiments, we demonstrate that the SKS model is, for all intents and purposes, unique. The idea is to show that a "small" change in the sketch results in a "small" change in the model. These experiments provide some experimental evidence to support Theorem 1.

Given two *distinct*—drawn by different individuals—sketches, we compute 50 intermediate sketches using linear interpolation. This allows us to consider 50 unique sketches and their corresponding models from one sketch to another. The measures used to to quantify the differences between the models and sketches respetively are the mean squared errors (MSEs):

$$MSE_{\mathcal{S}}(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2) = \sum_i (\boldsymbol{\alpha}_{1i} - \boldsymbol{\alpha}_{2i})^2 \tag{5}$$

$$MSE_{\mathcal{M}}(\boldsymbol{m}_1, \boldsymbol{m}_2) = \sum_j (\boldsymbol{m}_{1j} - \boldsymbol{m}_{2j})^2 . \tag{6}$$

We can observe how a change from the original sketch is reflected in the models by plotting the MSE of the models (Eq. (6)) with respect to the MSE for the sketches (Eq. (5)). In this case, the MSE is calculated using the interpolated sketch (model) and the original sketch (model). The expectation is that as the interpolated sketch differs from the original sketch (in terms of MSE), that the MSE between the models will also increase.

Some examples of this procedure are shown using projections of the higher dimensional models in Fig. 4. Notice how every perturbation of the sketch results in a corresponding change in the model, which is exactly what we imply when we say that model is (locally) unique. Some example plots of model MSE vs. sketch MSE are shown in Fig. 5.

5.2. Robustness

In the following experiment, we demonstrate the robustness of the accumulative framework. As in the previous section, we use the interpolation between two distinct sketches. While holding the model constant (i.e., let the model

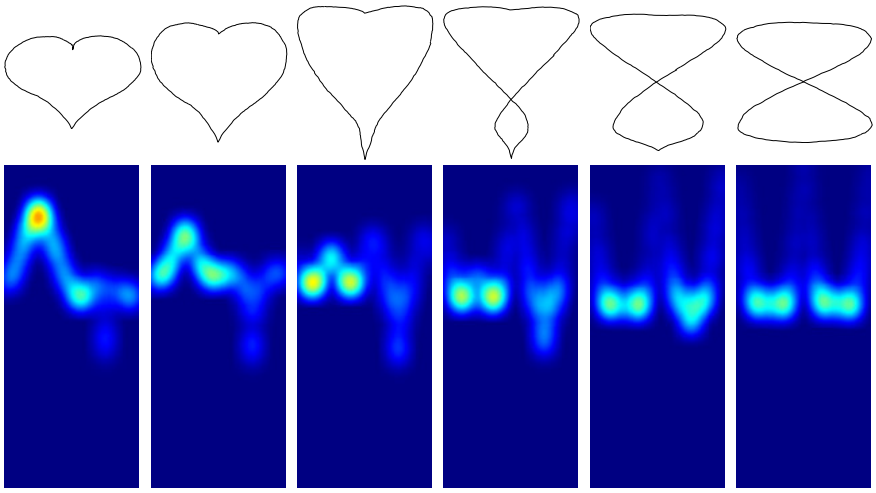


Figure 4: Shows the interpolation between a heart and a figure-8 (row 1). Then, the corresponding projections of the models onto the ρ-s plane are shown in row 2. Here, we can see that the first two shapes (and models) are more similar than the first and the last.

be constructed from the first in the interpolated sequence), let the login sketch vary. As the sketch differs, the accumulator peak changes too. Initially, the difference between the accumulator peaks is very little. As the sketch differs more and more, the accumulator peak becomes less distinctive, indicating less similarity between sketches. Therefore, despite small perturbations (from the sketch producing the model) occurring, the accumulator will still exhibit a sufficiently larger peak, indicating a matching sketch. This implies that the matching procedure is intentionally fuzzy, which makes the system more robust.

A sequence of test shapes and the accumulators are shown in Fig. 6.

5.3. DooDB Database

In this set of experiments, we use the DooDB database [28, 29], which contains a set of finger-drawn doodles (or sketches) and pseudo-signatures. For the purposes of comparing our system with a state-of-the-art method, we outline our experiments in the same manner.

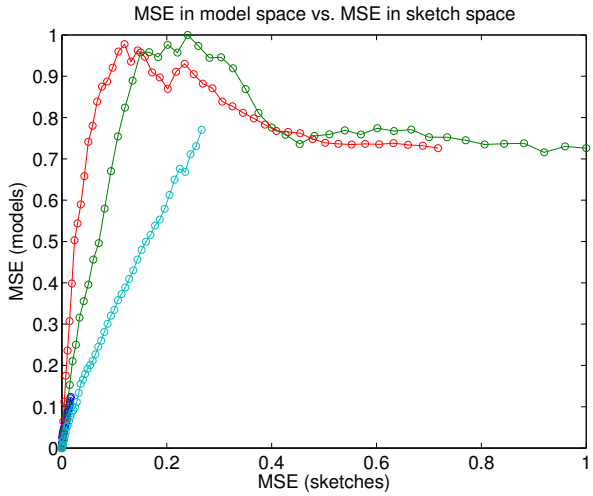


Figure 5: The plot shows how the MSE in the "space of sketches" is reflected in the "space of models" for the interpolation from one sketch to 4 different sketches. Initially, the MSE is null for both because the sketches and models are identical. However, as the sketches becomes different, the models also become increasingly different which is reflected in the examples shown here. The exact nature of the curve depends on both starting point and ending point in the "space of sketches."

The DooDB database contains files which include both spatial and temporal information, which are used for positional, velocity, and acceleration type features. Since their data was collected using a device with a resistive touch screen and without any hardware for detecting pressure, they do not use pressure as a biometric feature. Therefore, to compare the systems on a level playing field, our system is tested on the DooDB database without the biometric pressure. We will demonstrate the advantage of using biometric pressure in Section 5.4.

The performance of our SKS-based method is compared with the method used in [29], which is a Dynamic Time Warping (DTW) based system. They test performance on both doodles (or sketches) and pseudo-signatures, and they report an EER for both random and skilled forgeries (with the expectation that

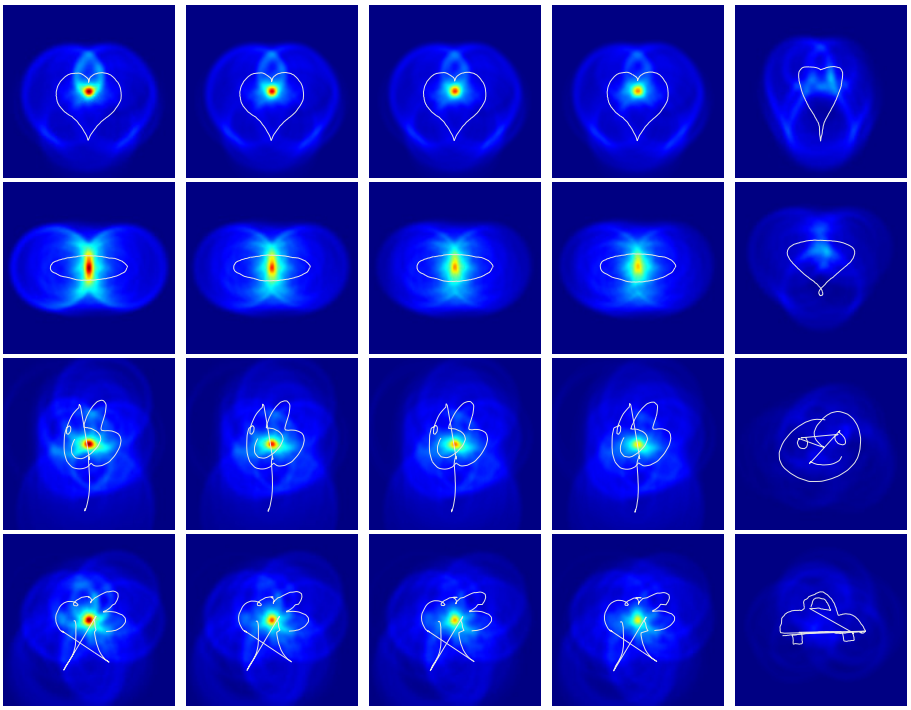


Figure 6: The test sketch is overlaid on the accumulator in order to show how the accumulator changes as the shape is deformed. Notice, how even deformed versions of the same sketch reveal a peak in the accumulator (columns 1–4). However, if the sketch is deformed too much the peak is diminished (column 5).

skilled forgeries will have worse performance). The performance measures used are the random forgery EER (denoted as EER_{rd}) and skilled forgery[2] EER (denoted as EER_{sk}) for both doodles and pseudo-signatures.

The results from [29] and our results are both reported in Table 1 for comparison. In [29], three different features sets are used with the DTW method. These features are ATVS-Pos, ATVS-Vel, and ATVS-Acc, which represent the spatial coordinates, velocity, and acceleration features respectively.

[2] A skilled forgery is defined as one in which the forger knows what the sketch looks like as well as its beginning and ending points

		Doodles		Pseudo-signatures	
Method	Session	EER_{rd}	EER_{sk}	EER_{rd}	EER_{sk}
ATVS-Pos	1	2.7	28.0	3.5	28.6
ATVS-Vel	1	3.4	**26.7**	**1.6**	23.9
ATVS-Acc	1	4.5	28.1	2.2	**19.8**
SKS	1	**1.4**	28.0	**1.6**	23.3
ATVS-Pos	2	7.6	36.4	5.0	34.5
ATVS-Vel	2	6.3	**33.9**	**3.8**	29.7
ATVS-Acc	2	7.3	34.1	4.3	**25.0**
SKS	2	**3.8**	35.9	5.2	28.5

Table 1: Performance comparison between DTW and SKS on DooDB database, which included both doodles and pseudo-signatures. The best performance is achieved using the SKS-Bio, which is the approach presented in this paper.

The results in Table 1 show that even *without biometric pressure* SKS is comparable to (better than in some cases) the DTW method. However, there are some important observations to note. First, SKS appears to perform slightly better than DTW on the doodles, but not on the pseudo-signatures. Recognizing doodles (or sketches) was the objective of our approach, and we have achieved an improved results on the set of doodles. For the pseudo-signature, we still achieve comparable performance to the DTW approach, despite not designing the system with signatures in mind. Second, but probably most significant, is that our system is easily generalized to incorporate features such as biometric pressure as a property of a sketch. Since the DooDB database does not have pressure, we cannot accurately compare the two systems using pressure. However, we believe that biometric pressure significantly improves performance over those systems without it. Finally, the DTW warping approach tests both velocities and accelerations. In our experiments, we found that the improvement from velocity came more from the direction than the magnitude (or speed). Now, acceleration, which is a second derivative with respect to time, is a very

noisy feature. In some cases, acceleration improves performance and in others acceleration worsens it.

5.4. Biometric Pressure

The following set of experiments aims to demonstrate the potential security benefit from adding biometric pressure to sketch-based password systems. A total of 100 sketches (with pressure information) from 5 different users were obtained using a Samsung Galaxy Note 10.1. Each of the 5 users provided 10 genuine sketches (i.e. 50 genuine sketches in total), and the remainder of the 100 sketches were skilled forgeries. Similar to the experiments performed on the DooDB database, we build a model using 3–5 example sketches (the first 3–5 sketches provided) and measure the verification performances (in terms of EER_{rd} and EER_{sk}) on the remaining sketches. The results are shown in Table 2.

Method	# Examples	EER_{rd}	EER_{sk}
SKS	3	**2.5**	17.8
SKS-Press	3	3.5	**10.7**
SKS	4	**2.5**	16.6
SKS-Press	4	4.1	**3.7**
SKS	5	1.6	14.0
SKS-Press	5	**0.0**	**3.3**

Table 2: Performance comparison between the sketch-based password system with and without biometric pressure. Observe how the pressure makes an improvement in performance in almost all cases: all skilled forgery scenarios, and the 5 example case for random forgeries.

The performance difference between SKS without pressure (SKS) and SKS with pressure (SKS-Press) is substantial; a more than 12% reduction in EER. The performance improvement for the random forgery scenario is less significant than that of the skilled forgery scenario. This is reasonable because in the

random forgery case, the shape and directional components of the sketch are already mostly distinct. Thus, there is not much to improve upon. However, for skilled forgeries the shape and direction components are as similar as humanly possible. Therefore, we can attribute the performances differences between SKS and SKS-Press to the biometric pressure. In every skilled forgery scenario tested: 3, 4, and 5 example sketches, the best performance is achieved by the addition of pressure.

6. Conclusions

In this paper, we discussed a novel sketch-based password system incorporating shape and the biometric pressure. Using an extension of the SKS shape recognition algorithm, we analyzed both the security and usability aspects of the approach. It was demonstrated that the model of a sketch is unique in the limit; implying a perfect security scenario. However, it was also shown by relaxing the smoothing matrix, we were able to balance both security with usability. The fuzziness that is built into the model of a sketch by means of the smoothing matrix directly affects the robustness and usability of authentication system.

The system, without using biometrics, was compared with a state-of-the-art DTW approach using the same database of pseudo-signatures and doodles (or sketches). In general, the SKS achieves similar performances (better in some cases). The advantage of SKS is the fact that it is more general than DTW. DTW requires restrictions such as boundary and monotonic constraints, where as SKS is robust to the start/end points and does not impose any monotonicity constraints. Thus, freeing SKS to accumulate evidence of consistency between sketch and model by means of more general transformations, opposed to the constrained method used by DTW.

More importantly, the addition of biometric pressure was shown to increase the level of performance by more than 12%. In security sensitive applications, the results demonstrate the potential for biometric pressure to provide improved security compared with sketch-based passwords that do not include this feature.

The average person is capable of reproducing a simple sketch with biometric pressure within a certain degree accuracy. However, there are still many questions to answer about using pressure for sketch-based passwords.

6.1. Future Work

In the future, we hope to construct a larger dataset that consists of sketches with biometric pressure in order to further demonstrate the security and usability improvement by using this feature. To our knowledge, there is no such sketch-based database that includes this information at this time. Therefore, we plan on making one publicly available.

Additionally, we hope combine the approach used in this paper with parameter estimation and feature selection. The addition of parameter estimation will hopefully provide improved results by having a variable smoothing parameter opposed to static one. Feature selection methods, such as KPCA, PCA, or ICA, provide the means to utilize the most meaningful features, which will provide a more compact and useful descriptor for a sketch-based password.

Acknowledgements

The information in this paper is based on work funded by the United States Army Research Office (ARO) grant W911NF-04-D-0003-0019.

References

[1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, J. M. Smith, Smudge attacks on smartphone touch screens, Proc. of the USENIX 4th Workshop on Offensive Tech. (2010) 1–7.

[2] P. Dunphy, J. Yan, Do background images improve draw a secret graphical passwords?, Proc. of the 14th ACM Conf. on Computer and Communications Security (2007) 36–47.

[3] M. Oka, K. Kato, Y. Xu, L. Liang, F. Wen, Scribble-a-secret: Similarity-based password authentication, 19th Int'l Conf. on Pattern Recognition (2008) 1–4.

[4] R. Dhamija, A. Perrig, Déjà vu: A user study using images for authentication, Proc. of the 9th USENIX Security Symposium (2000) 45–58.

[5] . PASSFACES CORPORATION, The science behind passfaces, `http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf`, 2009.

[6] S. Weidenbeck, J. Waters, J. Birget, A. Brodskiy, N. Memon, Authentication using graphical passwords: Basic results, Proc. of the 11th Int'l Conf. on Human-Computer Interaction (2005).

[7] S. Weidenbeck, J. Waters, J. Birget, A. Brodskiy, N. Memon, Authentication using graphical passwords: Effects of tolerance and image choice, Proc. of the 1st Symposium on Usable Privacy and Security (2005) 1–12.

[8] S. Weidenbeck, J. Waters, J. Birget, A. Brodskiy, N. Memon, Passpoints: Design and longitudinal evaluation of a graphical password system, Int'l Journal of Human Computer Studies 63 (2005) 102–127.

[9] A. De Angeli, L. Coventry, G. Johnson, K. Renaud, Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems, Int'l Journal of Human Computer Studies 63 (2005) 128–152.

[10] K. V. Renaud, Guidelines for designing graphical authentication mechanism interfaces, Int'l Journal of Information and Computer Security 3 (2009) 60–85.

[11] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin, The design and analysis of graphical passwords, Proc. of the 8th USENIX Security Symposium (1999) 1–14.

[12] H. Gao, X. Guo, X. Chen, L. Wang, X. Liu, Yet another graphical password strategy, Proc. of the Annual Computer Security Applications Conference (2008) 121–129.

[13] J. Goldberg, J. Hagman, Doodling our way to better authentication, Proc. of the ACM Conference on Human Factors in Computing Systems (2002) 868–869.

[14] C. Varenhorst, Passdoodles: A lightweight authentication method, MIT Research Science Institute (2004).

[15] H. Tao, C. Adams, Pass-go: A proposal to improve the usability of graphical passwords, Int'l Journal of Network Security 7 (2008) 273–292.

[16] D. Davis, F. Monrose, M. K. Reiter, On user choice in graphical password schemes, Proc. of the 13th USENIX Security Symposium (2004) 151–164.

[17] K. V. Renaud, On user involvement in production of images used in visual authentication, Journal of Visual Languages & Computing 20 (2009) 1–15.

[18] S. Chiasson, P. C. Van Oorschot, R. Biddle, Graphical password authentication using cued click points, 12th European Symposium on Research in Computer Society (2007) 359–374.

[19] S. Chiasson, A. Forget, R. Biddle, P. C. Van Oorschot, Influencing users towards better passwords: Persuasive cued click-points, British Computer Society Conference on Human-Computer Interaction 1 (2008) 121–130.

[20] R. Biddle, S. Chiasson, P. C. Van Oorschot, Graphical passwords: learning from the first twelve years, ACM Computing Surveys 44 (2012) 1–25.

[21] M. Fuandez-Zanuy, Biometric Security Technology, IEEE Aerospace and Electronic Systems Magazine 21 (2006) 15–26.

[22] A. K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Trans. on Circuits and Systems for Video Technology 14 (2004) 4–20.

[23] D. G. Kendall, Shape manifolds, procrustean metrics, and complex projective spaces, Bulletin London Math. Soc. 16 (1984) 81–121.

[24] W. E. Snyder, A strategy for shape recognition, in: A. Srivastava (Ed.), Workshop on Challenges and Opportunities in Image Understanding, College Park, MD, 2007.

[25] K. Krish, S. Heinrich, W. E. Snyder, H. Cakir, S. Khorram, Global registration of overlapping images using accumulative image features, Pattern Recognition Letters 31 (2010) 112–118.

[26] K. Krish, An accumulative framework for object recognition, Ph.D. thesis, North Carolina State University, 2009.

[27] M. Rousson, D. Cremers, Efficient kernel density estimation of shape and intensity priors for level set segmentation, Medical Image Comput. and Comp.-Ass. Interv. (MICCAI) 1 (2005) 757–764.

[28] M. Martinez-Diaz, J. Fierrez, C. Martin-Diaz, J. Ortega-Garcia, DooDB: A Graphical Password Database Containing Doodles and Pseudo-Signatures, 12th Int'l. Conf. on Frontiers in Handwriting Recognition (2010) 339–344.

[29] M. Martinez-Diaz, J. Fierrez, J. Galbally, The DooDB Graphical Password Database: Data Analysis and Benchmark Results, IEEE Access 1 (2013) 596–605.